Attorney Docket No. AT03 0055 US1 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Ernst Haselsteiner et al. Group Art Unit: 2431

Application No.: 10/574,630 Examiner: Abrishamkar, Kaveh

Filed: May 12, 2008 Confirmation No.: 1877

For: METHOD OF AND CIRCUIT FOR IDENTIFYING AND/OR VERIFYING HARDWARE AND/OR SOFTWARE OF AN APPLIANCE AND OF A DATA CARRIER COOPERATING WITH THE APPLIANCE

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF UNDER 37 C.F.R. § 41.41 (a)

This is an appeal to the Board of Patent Appeals and Interferences from the decision of the Examiner dated June 4, 2009, which finally rejected claims 1-15 in the above-identified application. An Appeal Brief was filed on November 2, 2009. This Reply Brief is in response to the Examiner's Answer dated February 8, 2010. This Reply Brief is hereby submitted pursuant to 37 C.F.R. § 41.41 (a).

CERTIFICATE OF MAILING UNDER 37 C.F.R. 1.8

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Date:____________ Signed:______________________________

Typed Name: Mark A. Wilson

TABLE OF CONTENTS

I. STATUS OF CLAIMS

No claims are canceled.

No claims are withdrawn.

No claims are objected to.

Claims 1-15 stand rejected as follows:

Claims 1-15 stand rejected under 35 U.S.C. 102(a) as being anticipated by Proudler et al. (EP 1280042, hereinafter Proudler).

Claims 1-15 are the subject of this appeal. A copy of claims 1-15 is set forth in the Claims Appendix.

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-3 and 6 are patentable over Proudler under 35 U.S.C. 102(a).

B. Whether claim 4 is patentable over Proudler under 35 U.S.C. 102(a).

C. Whether claim 5 is patentable over Proudler under 35 U.S.C. 102(a).

D. Whether claims 7, 8, and 10-15 are patentable over Proudler under 35 U.S.C. 102(a).

E. Whether claim 9 is patentable over Proudler under 35 U.S.C. 102(a).

III. ARGUMENT

For the purposes of this appeal, claims 1-3 and 6 are argued together as a group for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 4 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 5 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claims 7, 8, and 10-15 are argued as a separate group for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a). Claim 9 is argued separately for purposes of the question of patentability over Proudler under 35 U.S.C. 102(a).

A. Claims 1-3 and 6 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims.

Appellants respectfully submit that claim 1 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Appellants appreciate the Examiner's clarification as to the specific teachings of Proudler that are relied on for the purported disclosure of the first and second units and the first and second authorization data. The following table summarizes the correlations asserted by the Examiner.

Claim Limitation	Asserted Disclosure of Proudler
First unit	**Measurement function 31.** The first unit is interpreted as being the measurement function of the trusted device (Figure 8, item 24, block 31: see paragraph 0029) which receives an integrity metric (authorization data from the computing platform (see paragraph 0029). Examiner's Answer, 2/8/10, pages 9-10.
First authorization data	**Integrity metric.** The second unit is interpreted as being the authentication function block of the trust[ed] device (Figure 8, item 24, block 33) which authenticates the smart card via encryption/decryption and signature/verification (second authorization data) (see paragraphs 0029-0030). Examiner's Answer, 2/8/10, page 10.
Second unit	**Authentication function 33.** As disclosed above, the first authorization data is the integrity metric transmitted from the computing platform (hardware) to the first unit (see paragraph 0029). Examiner's Answer, 2/8/10, page 10.
Second authorization data	**Authorization information.** The second authorization data is interpreted as the authentication information transmitted between the smart card and the second unit (see paragraphs 0029-0030). Examiner's Answer, 2/8/10, page 10.

In light of these specific correlations asserted by the Examiner, it is clear that Proudler does not disclose all of the limitations of the claim. For specific discussion, the following explanations show that Proudler fails to disclose the specific limitations which recite the first unit and the first authorization data. The discussion of these limitations should be sufficient and, hence, there is no need to discuss further the specific limitations which recite the second unit and the second authorization data.

1. Proudler does not disclose transmitting first authorization data of the hardware and/or software to a first unit.

Proudler does not disclose transmitting first authorization data of the hardware and/or software to a first unit, as recited in the claim. By way of comparison, using the asserted teachings of Proudler relied on for the rejection, Proudler does not disclose transmitting the integrity metric of the hardware and/or software to the measurement function 31.

Although Proudler generally describes the measurement function 31 acquiring the integrity metric from the computing platform 10, Proudler does not disclose transmitting the integrity metric from the computing platform 10 to the measurement function 31. Proudler merely describes the measurement function 31 measures or acquires the integrity metric of the computer platform 10. Proudler, paragraphs 29 and 33. The measurement function 31 has access to volatile memory 4 for storing the acquired integrity metric. Proudler, paragraph 34. As an example of how the measurement function 31 acquires the integrity metric, Proudler explains:

> In the present embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory.

Proudler, paragraph 33, lines 4-7 (emphasis added).

Thus, the term "acquire" as used in Proudler does not encompass transmitting because transmitting is not described or equivalent to the functionality of generating a digest of the BIOS instruction, as described in Proudler. Therefore, the assertion by the Examiner that the integrity metric is purportedly transmitted from the computing

platform 10 to the measurement function 31 is inaccurate and not supported by the actual disclosure of Proudler.

Moreover, the only transmission of the integrity metric that appears to be described in Proudler is <u>from</u> the trusted device 24 (which includes the measurement function 31) to the user. Proudler, paragraph 17. However, the description of transmitting the integrity metric from the trusted device 24 to the user does not support the Examiner's assertion that the integrity metric is purportedly transmitted from the computing platform 10 to the measurement function 31. Furthermore, the description of transmitting the integrity metric from the trusted device 24 to the user in insufficient to disclose transmitting the integrity metric from the computing platform 10 to the measurement function 31.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose transmitting first authorization data of the hardware and/or software to a first unit, as recited in the claim. More specifically, within the context of the rejection, Proudler does not disclose transmitting the integrity metric from the computing platform 10 to the measurement function. Accordingly, Appellants respectfully assert claim 1 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

2. <u>Proudler does not disclose comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit.</u>

Proudler does not disclose comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit, as recited in the claim. By way of comparison, using the asserted teachings of Proudler relied on for the rejection, Proudler does not disclose comparing the <u>integrity metric</u> of the hardware and/or software that has been transmitted to the <u>measurement function 31</u> with first verification data stored in the <u>measurement function 31</u>. For a more complete contextual understanding, it appears that a further correlation is intended between i) the recited first verification data recited in the claim, and ii) the expected values described in Proudler.

Despite the assertions in the Examiner's Answer, the measurement function 31 does not store the expected values (the first verification data) that are compared with the integrity metric. Rather, the comparison is performed by the user, and the user receives the expected values from the trusted party—not from the trusted device 24. In particular, the identity and integrity metric are requested and received by the user from the trusted device compared, and the user compares the identity and integrity metric from the trusted device with the expected values from the trusted party. Proudler, paragraphs 16-17. So there is no disclosure of storing the expected values at the trusted device 24 or, more specifically, in the measurement function 31 of the trusted device 24. Therefore, the implications of the assertion by the Examiner that the integrity metric is compared with first verification data purportedly stored in the measurement function is inaccurate and not supported by the actual disclosure of Proudler.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit, as recited in the claim. More specifically, within the context of the rejection, Proudler does not disclose comparing the integrity metric of the hardware and/or software that has been transmitted to the measurement function 31 with first verification data stored in the measurement function 31. Accordingly, Appellants respectfully assert claim 1 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

3. <u>Proudler does not disclose authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit.</u>

Proudler does not disclose authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit, as recited in the claim. By way of comparison, using the asserted teachings of Proudler relied on for the rejection, Proudler does not disclose authorizing the hardware and/or

software once it has been ascertained that there is coincidence between the <u>integrity metric</u> provided by the hardware and/or software and the first verification data stored in the <u>measurement function 31</u>.

As explained above, the measurement function 31 does not store the expected values (apparently corresponding to the first verification data) from the trusted party. Since Proudler does not disclose storing the expected values in the measurement function 31, Proudler cannot disclose ascertaining that there is coincidence between the integrity metric and expected values stored in the measurement function.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit, as recited in the claim. More specifically, within the context of the rejection, Proudler does not disclose authorizing the hardware and/or software once it has been ascertained that there is coincidence between the integrity metric provided by the hardware and/or software and the first verification data stored in the measurement function 31. Accordingly, Appellants respectfully assert claim 1 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

4. <u>Proudler does not disclose a direct data exchange is carried out between the first unit and the second unit.</u>

Proudler does not disclose a direct data exchange is carried out between the first unit and the second unit, as recited in the claim. By way of comparison, using the asserted teachings of Proudler relied on for the rejection, Proudler does not disclose a direct data exchange is carried out between the <u>measurement function 31</u> and the <u>authentication function 33</u>.

As a preliminary matter, it should be noted that this assertion is inconsistent with the previous assertions presented by the Examiner for this language of the claim. Previously, the Examiner had relied on disclosure of communication between the trusted device 24 and the computing platform 10. However, both of the measurement function 31 and the authentication function 33 currently relied on are components within the

trusted device 24, so there appears to be no further reliance on the communications between the trusted device 24 and the computing platform 10.

Nevertheless, regardless of this and other inconsistencies in the Examiner's assertions, Proudler does not disclose a direct data exchange between the measurement function 31 and the authentication function 33. In fact, Proudler appears to be silent in regard to any type of potential communications, or functionality for performing such communications, between the measurement module 31 and the authentication module 33. Furthermore, there appears to be no need for or benefit from such communications between the measurement module 31 and the authentication module 33, within the context of Proudler. Therefore, Proudler simply does not address or disclose a direct data exchange between the measurement function 31 and the authentication function 33.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose a direct data exchange is carried out between the first unit and the second unit, as recited in the claim. More specifically, within the context of the rejection, Proudler does not disclose a direct data exchange between the measurement function 31 and the authentication function 33. Accordingly, Appellants respectfully assert claim 1 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claims 2-6 depend from and incorporate all of the limitations of independent claim 1, which is patentable over the cited references, Appellants respectfully submit that these claims are also patentable over the cited reference based on an allowable base claim. Additionally, each of these claims may be allowable for further reasons. Accordingly, Appellants request that the rejections of claims 2-6 under 35 U.S.C. 102(a) be withdrawn.

B. Claim 4 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claim 4 depends from and incorporates all of the limitations of independent claim 1, which is patentable over Proudler, Appellants respectfully submit that dependent claim 4 is also patentable over Proudler based on an allowable base claim.

Additionally, claim 4 is patentable over Proudler for further reasons, as explained in the Appeal Brief filed previously.

C. <u>Claim 5 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.</u>

Given that claim 5 depends from and incorporates all of the limitations of independent claim 1, which is patentable over Proudler, Appellants respectfully submit that dependent claim 5 is also patentable over Proudler based on an allowable base claim. Additionally, claim 5 is patentable over Proudler for further reasons, as explained in the Appeal Brief filed previously.

D. <u>Claims 7, 8, and 10-15 are patentable over Proudler because Proudler does not disclose all of the limitations of the claims.</u>

Appellants respectfully submit that claim 7 is patentable over Proudler because Proudler does not disclose all the limitations of the claim. Claim 7 recites:

> A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the circuit comprising:
>
> a first unit for identifying and/or verifying the hardware and/or software of the appliance, comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified, and
>
> a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software,
>
> wherein <u>a communication interface is provided between the central arithmetic units of the first unit and the second unit</u>.

(Emphasis added.)

In addition to the arguments explained in the Appeal Brief filed previously, Proudler further does not disclose a communication interface is provided between the central arithmetic units of the first unit and the second unit, where the first and second units are asserted to be the measurement function 31 and the authentication function 33, respectively. In fact, there is no disclosure in Proudler of the measurement function 31 (asserted as the first unit) having a central arithmetic unit. Similarly, there is no

disclosure in Proudler of the authentication function 33 (asserted as the second unit) having a central arithmetic unit. Consequently, Proudler cannot and does not disclose a communication interface between the measurement module 31 and the authentication module 33.

For the reasons presented above, Proudler does not disclose all of the limitations of the claim because Proudler does not disclose a communication interface is provided between the central arithmetic units of the first unit and the second unit, as recited in the claim. More specifically, within the context of the rejection, Proudler does not disclose a communication interface is provided between the central arithmetic units of the measurement function 31 and the authentication function 33. Accordingly, Appellants respectfully assert claim 7 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claims 8-15 depend from and incorporate all of the limitations of independent claim 7, which is patentable over the cited references, Appellants respectfully submit that these claims are also patentable over the cited reference based on an allowable base claim. Additionally, each of these claims may be allowable for further reasons. Accordingly, Appellants request that the rejections of claims 7-15 under 35 U.S.C. 102(a) be withdrawn.

E. Claim 9 is patentable over Proudler because Proudler does not disclose all of the limitations of the claim.

Given that claim 9 depends from and incorporates all of the limitations of independent claim 7, which is patentable over Proudler, Appellants respectfully submit that dependent claim 9 is also patentable over Proudler based on an allowable base claim. Additionally, claim 9 is patentable over Proudler for further reasons, as explained in the Appeal Brief filed previously.

IV. CONCLUSION

For the reasons stated above, claims 1-15 are patentable over the cited references. Thus, the rejections of claims 1-15 should be withdrawn. Appellants respectfully request that the Board reverse the rejections of claims 1-15 under 35 U.S.C. 102 (a).

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account **50-4019** pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account **50-4019** under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21.

Respectfully submitted,

/mark a. wilson/

Date: April 7, 2010

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111

V. CLAIMS APPENDIX

1. A method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the method comprising:

transmitting first authorization data of the hardware and/or software to a first unit,

comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit,

authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit,

transmitting second authorization data of a data carrier to a second unit,

comparing the second authorization data in the second unit with second verification data stored in the second unit, and

authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit,

wherein a direct data exchange is carried out between the first unit and the second unit.

2. A method as claimed in claim 1, wherein the direct data exchange between the first unit and the second unit comprises a transmission of encrypted data and a comparison and/or decryption of data transmitted between the first unit and the second unit.

3. A method as claimed in claim 1, wherein the data exchange between the first unit and the second unit is carried out prior to an identification and/or verification of first authorization data of the hardware and/or software and of second authorization data of the data carrier.

4. A method as claimed in claim 1, wherein a central arithmetic unit of the first unit and a central arithmetic unit of the second unit jointly access at least one ROM memory one RAM memory and/or one non-volatile memory.

5. A method as claimed in claim 1, wherein encryption of the first authorization data and of the second authorization data is carried out in the first unit and in the second unit.

6. A method as claimed in claim 1, wherein the second authorization data are obtained from a smartcard or a tag or a label that forms the data carrier.

7. A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, the circuit comprising:

a first unit for identifying and/or verifying the hardware and/or software of the appliance, comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified, and

a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software,

wherein a communication interface is provided between the central arithmetic units of the first unit and the second unit.

8. A circuit as claimed in claim 7, wherein the memories of the first unit and of the second unit are formed by a ROM memory and a RAM memory and/or a non-volatile memory.

9. A circuit as claimed in claim 7, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory.

10. A circuit as claimed in claim 7, wherein the first unit and the second unit in each case comprise an encryption device.

11. A circuit as claimed in claim 7, wherein the central arithmetic unit of the first unit and the central arithmetic unit of the second unit are combined to form a common central arithmetic unit which common central arithmetic unit has the integrated communication interface, and wherein the common central arithmetic unit is connected by an interface to the hardware and/or software that is to be identified and/or verified.

12. A circuit as claimed in claim 7, wherein the interface to the external data carrier is designed for contactless communication with the external data carrier.

13. A circuit as claimed in claim 7, wherein the external data carrier is formed by a smartcard or a tag or a label.

14. An appliance which comprises as hardware at least one central arithmetic unit which central arithmetic unit is designed to run software and to obtain data from an external data carrier cooperating with the appliance, wherein a circuit as claimed in claim 7 is coupled to the central arithmetic unit.

15. An appliance as claimed in claim 14, wherein the central arithmetic unit of the appliance is coupled via an interface integrated in the central arithmetic unit of the appliance to the circuit integrated in the central arithmetic unit.